Arid Zone Journal of Engineering, Technology and Environment, December, 2017; Vol. 13(6):801-809

Print ISSN: 1596-2490, Electronic ISSN: 2545-5818, www.azojete.com.ng

Security Architecture for Thin Client Network

O. A. Okunade

Department of Computer Science, Faculty of Sciences, National Open University of Nigeria (NOUN), Cadastral Zone, Nnamdi Azikiwe Expressway, Jabi, Abuja, Nigeria.

Corresponding Author's email address: aokunade@noun.edu.ng

Abstract

Client-server is a modern shift in computing paradigm that different from traditional (pc-server) computing in the sense that data resides remotely on the server, this makes centralized management data possible. Client-server has an edge over traditional computing model in the areas of functionality, performance, and reliability. Client computing has become cost effective and centrally managed network. It reduces total cost of ownership (TCO) to a great extent improved services and lower power usage in comparison to pc-server computing model. However, there are security challenges facing client-server computing such as inability for security solution to identify user based on its static type of IP address. This paper presents Dynamic Host Control Protocol (DHCP) as a remedy to challenges associated with dynamic assignment of IP address. These enable to detect spoofing of MAC address with login parameters that does not match information in the server, when an attacker tries to "break in", using inconsistent parameters, the MAC address in which an IP is assigned will mismatch and as a result there would be an IP address conflict detected by the administrator. The design thin-client network framework help to overcome the identified security challenges of client-server network.

Key Words: thin client, security challenge, user management, client-server.

1.0 Introduction

Thin client computing is an ideal computing paradigm; but not without challenges. This paper focuses on security challenges associated with thin client computing: Security is the most important issue in client-server computing. According to Rajesh and Umesh (2012) security concerns are number one issue facing clouds (client) computing. IP Address is always static (same) for all users that is the terminal server's IP addresses. The security enforcer solution finds it difficult to differentiate the user's request as it always see same IP addresses in all type of requests coming from terminal, as such identifying users becomes a challenge Carl and Guynes (2011). Thin Client / Server Architecture, which has been one of the hot topics in the information systems literature for the last decade, nowadays, becomes a powerful, secure and cost-efficient solution for health, finance, education and other industrial sectors. For instance, several public/private companies/institutions have tendency for cloud computing, virtualization, and so on, to keep up with the speed of hardware/software technology development, and improves the preference of client / server architecture.

Thin clients improve information system efficiency at several institutions, in client / server architecture, software and data are stored in the remote servers on the network. However, it is possible to communicate and exchange data with other clients on the network. User data is stored on the remote file servers on the network. Software upgrade is done remotely on the network. Thin clients have more lifetimes according to personal computers as they have less vulnerable hardware parts (Yusuf and Halit, 2014). Moreover, it is easier to use thin clients as they have

standard software and user interface all over the related institution. In addition to this, ease of thin client installation makes recovery in case of system crash faster and lessens the need for technical assistance. Information and data security can be improved with the usage of thin clients. As they do not have local disks or portable media drives, they are less vulnerable to viruses and spy wares. Users can only store data on remote file servers and cannot copy or move critical data to a portable media. The usage of thin clients in a domain on the network makes system administration easier and safer with respect to the remote user control and system policy checking in the domain that lessens the system internal threats. Thin client / server architecture is a cost-efficient information system infrastructure; it is cheaper and has less hardware parts and more lifetimes. At the same time, system management and maintenance is easier as software upgrade and data storage/backup are done on remote servers. Finally, thin clients have less power consumption than personal computers (Lee, Kim and Kim, 2015). According to the mentioned characteristics, a detailed comparison of thin clients and personal computers with respect to several criteria are summarized in Table 1.

Table 1: Comparison of PC (Personal Computer) and Thin Client with Respect to Several Criteria. (Cimen, *et al.*, 2014)

Criteria	**Personal Computer (PC)**	**Thin Client**
Operating System	Manual installation on local disk	Installed on flash memory (DOM). No need for manual installation
Anti-Virus protection	Needs Anti-Virus protection software	No need for anti-virus protection portable media
Software Upgrade	Needs for manual software upgrade periodically	No need for manual software upgrade. Only remote software upgrade
System	Risk for system crash according to users fault	Remote system recovery in case of system crash

Thin client/server architecture has a prominent advantage in terms of power consumption, it reduced power usage by 24%, carbon dioxide emission by 23% and increase the life span by five to ten years, by replacing desktops by thin clients, nearly two-thirds of the power consumption can be reduced (Davis, 2008). Thin client / server architecture is used by educational institutions as they allow students to analyze real data in their research without modifying or removing data either deliberately or unconsciously (Hatakeyama, *et al.*, 2011). Also, this architecture disallows unauthorized access to critical data from outside the institution. Moreover, computer-aided education has overlapping characteristics with thin client/server architecture in terms of multiple usages of digital resources and cost-effectiveness (Reynolds, 2006). Lots of benefits of cloud computing in education, for example provision of educational resource storage and databases, e mails, educational applications and tools for students and teachers and clients located all over the world involving in an educational program and advantages in cost for improving the quality of system in terms of Total Cost of Ownership (Anwar and Xiaodi, 2012). This encourages the use of thin clients in several implementation areas and has renewed people's interest in the thin client concept (Deboosere, *et al.*, 2007).

1.1 Thin-Client Computing Model

Fundamental approach behind thin-client computing is that it runs application centrally with only keyboard, video and mouse (KVM) updates transmitted across the network, instead of running applications locally on PCs with all of their associated challenges and costs. Bandwidth usage is minimal compared to traditional PC/server environments, with wireless LAN being ideal for the clients. The server backbone linking the terminal servers, data servers, mail servers, and so on, is the only LAN connection that needs high capacity. In a traditional fat-client environment, applications are stored locally and data is stored centrally, when a file is opened, the entire file is transferred to the local PC, with the results being saved back across the LAN/WAN to the central storage area. Server/client architecture (such as SQL and Oracle), handle this process slightly differently, but processing still takes place at the local PC. This requires high bandwidth to each PC. The thin-client/server architecture enables 100 percent server-based processing, management, deployment, and support for mission-critical, productivity, Web-based, or other custom applications across any type of connection to any type of client hardware, regardless of platform (Barrie, 2002).

1.2 Bandwidth and physical characteristics client

The thin-client itself takes up almost no space, it measures about seven inches long, five inches wide, 1.4 inches tall, and weighs about six 2.72kilogram (see Figure 3). Physical Characteristics of Wyse S90 Model Thin-client, design tested by the authors mounted directly to the back of 17 inches flat panel monitor as shown in Figure 1, Wyse 2007. Wyse S90 Mounted on the Back of a LCD monitor compared to the space required for a standard desktop PC, which has a tower cabinet in addition to the monitor that sits either under the desk or alongside the monitor, the space saved can be better utilized for other purposes or storage. Using thin-clients essentially reduces the footprint of the workstation to that of the monitor.

Figure 1: Physical Characteristics of the Wyse S90 Model Thin-client (Wyse Technology Web site, 2007).

Physical characteristics of a thin-client are as follow:

Height	1.38 inches (34mm)
Width	6.94 inches (177mm)

Depth	4.75 inches (121mm)
Shipping Weight	6 ibs8 inches (2.7kg)

The design tested by the author mounted directly to the back of 17inches flat panel monitor shown in figure 2.

Figure 2: Wyse S90 Mounted on the Back of a LCD Monitor
(Wyse Technology, 2007)

Additionally, thin-clients use less network bandwidth. Rather than clogging up bandwidth with redundant files on the LAN, PC, and printer, the thin-client's document or program is only opened and processed at the server and then sent to the printer if necessary. In a thin-client environment, only mouse movements, key strokes, and screen updates are transmitted from one end-user to another. A Microsoft Corporation study conducted by NEC and Group Bull showed that structured task workers are the highest bandwidth users as they generally perform the same tasks over and over again. These workers used up about 20 kilo-bits of bandwidth apiece, sending documents back and forth to different stations around the network or to the centralized network printer. A study of a 130-user tubby-client network in the United Kingdom yielded the following results in regards to bandwidth consumption: Table 2. Shows the average Bandwidth used by client type. The table 2 shows that the bandwidth used by tubby clients is less than that of fat clients. The bandwidth consumption is even less for a thin client network and the net effect is that far less bandwidth is needed and used by each user to support routine daily operations and will likely result in lower server costs and LAN sizes since not as much speed in megabytes per second (Mbps) will be needed and a less expensive LAN will be required to accommodate increased file transfer needs and e-mail storage (Barrie, 2002).

Table 2: Thin Client bandwidth Consumption (Lawton, 2007)

Bandwidth Utilisation	Average bandwidth utilization	Peak bandwidth utilization
Fat Client	40%	80%
Tubby Client	0.5%	4%

The net effect is that far less bandwidth is required for remote and local sites, further reducing costs in multi-site installations.

1.3 Thin-Client/Server Computing

According to Joel (2005) shown in figure 1, thin-client/server computing model involves connecting thin-client software or a thin-client hardware device with the server side using a highly efficient network protocol such as Citrix's ICA. The thin-client/server architecture enables

100 percent server-based processing, management, deployment, and support for mission-critical, productivity, Web-based, or other custom applications across any type of connection to any type of client hardware, regardless of platform. The client hardware can include Windows-based terminals, PCs, Net PCs, network computers, Apple Macintosh computers, or UNIX devices. Using the thin-client/server computing model, you will not need to purchase or upgrade hardware just to run the latest software--instead, you will be able to let it comfortably evolve, leveraging your existing hardware, operating systems, software, networks, and standards. Thin-client/server computing extends the life of your computing infrastructure considerably.

2.0 Materials and Methodology

Dynamic host control protocols are applied to solve the security challenges of thin client. First, the client was connected to the server over TCP/IPv4; client requests an IP address from the server, servers in turn ask for a dynamic IP address over TCP/IP from a router, router assign an IP address dynamically to the server, server then serves the request of the client. Then the network is connected to a managed Users Threat Management switch (UTMs). With dynamic IP address assigned by the router, the administrator can authenticate and monitor the activities of the user over the network. This method uses a single request and response technique, although at times the device opens a persistent TCP connection with more than one request being transported with a TCP session. This method of request and access right is illustrated in figure 3.

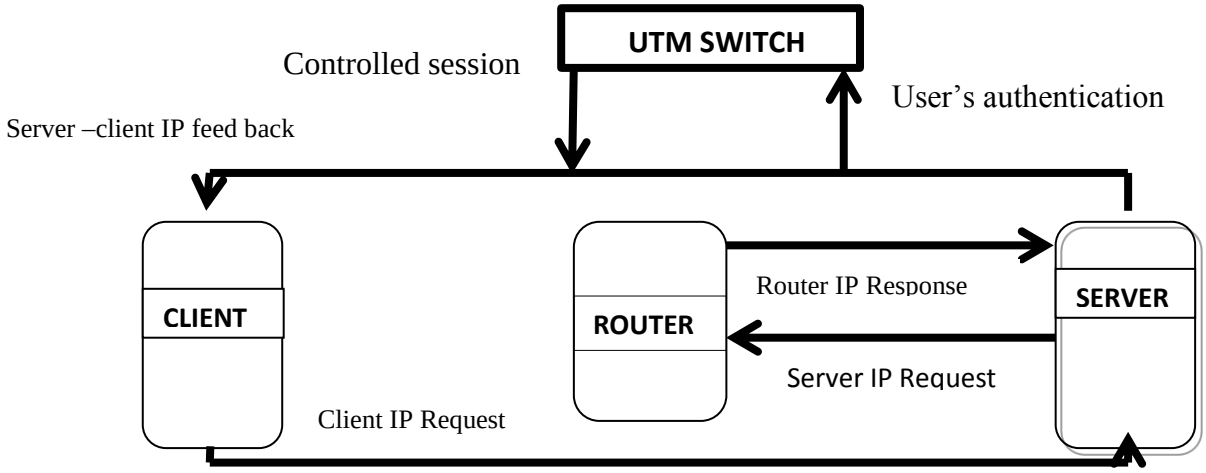

Figure 3: IPv4 running on DHCP

Because of the fact that static IP makes it difficult for security solution to enforce it defense against attacker since the server sees all users as the same. Dynamic Host Control Protocol (DHCP) is one of the most common means that can provide remedy to these challenges. This dynamically assigns IP addresses to clients as they connect to the network. In many cases, the server will assign an IP address to any client which asks for one, that is available user at a given point in time (Jonathon, et al., 2004). In a slightly more secure setup, the DHCP server can be setup to deny an IP address to any client whose MAC address is not known, and if desired can

give a specific IP address (and often an associated hostname) to those known MAC addresses. This provides a measure of protection. Another "layer" to defense, "human layer" can prevent clients who can spoof a MAC address from connecting. In a thin client environment, this is less of a worry, as the MAC spoofing generally is done after an OS is up and running, not during the early stages of the OS boot process. Since thin clients get their OS from a central server, the user has little opportunity to alter their MAC address. Of course, this does little to prevent a user from walking into the office with his personal laptop and connecting to the network, if he or she chooses to spoof a MAC address (Robison et al., 2004). Because most client requests are "broadcast" requests (sent to address 0.0.0.0, and thus "heard" by all network connections on the network) it is a trivial matter for a non-trusted DHCP server to answer the request and provide network information to the booting client, as well as a non-trusted kernel image for the client to boot from using trivial file transfer protocol. Because of this broadcast nature, it is important to have a routers block broadcast requests outside of the subnet from where they originated. Therefore, an attacker who wants to emulate a DHCP server will need access to the subnet itself.

Note: Dynamic Host Control Protocol is the protocol on which the network runs. The function of DHCP is to enable the router to dynamically assign IP address to the client(s). See fig 3.

3.0 Results and Discussions

Attacker who tries to spoof the MAC address with his login parameters that does not match information in the server can be detected. When an attacker tries to "break in", using inconsistent parameters, the MAC address in which an IP is assigned will mismatch and as a result there would be an IP address conflict which is detected by the administrator. It is important that the network is design in segments. A segment having number given of clients say 20 to 30 clients assigned to one segment of the network under a particular user account created in the server. This will enable the administrator to know what segment of the network a hacker is located. This is a deviation from the approach of assigning a static IP to a client. Because an attacker can walk up to a system (client), guess a static IP address and if he guess write and is authenticated, can gain access the resources and steal/manipulate valuable data. All the users' data, applications and Operating System (OS) will be stored in the server only; nothing will be stored in the user's desktops. This means when the user logs on to his/her desktop, that particular user's applications, data and Operating System will be loaded on to the desktop from the server. Users who may be geographically scattered can access their data from the server once they are connected to their LAN. Thin client Virtualization solutions are provided by VMware, Wyse, Citrix and Sun VDI. For this paper VMware's desktop virtualization was used for implementing the network. Thin client virtualization has shown maximum performance for the organization that has used it. This technology allows the network administrators to administer, control, manage and maintain many user desktops on a single, central computer or server. Overall costs required for maintaining and upgrading the network are drastically reduced, thereby reducing the number of hardware and increasing the server's performance. Thin client Virtualization has improved desktop

management and control with faster deployment of desktops and fewer IT support calls. This technology has proved to be the best thin-client solution giving the organizations networks the highest availability and performance and reducing capital costs.

For desktop virtualization to work Fig 4, desktop virtualization software needs to be installed on the server. When a user logs on to his computer using his username and password, the user's credentials is sent for authentication to the Active Directory domain services. Once logged on, the user is allotted his virtual machine, which is nothing but a client PC, from the list of client IP addresses available. Both guest and host Operating Systems have to be installed on the virtual machine in order to make it work. Guest and host Operating System is useful if the virtual machine is being shared by more than one user. The user can switch between the Operating System of his choice by just choosing the OS and logging into the system. The working behind desktop virtualization is as follows: A Virtual Machine (Fig 4 and 5) image file is created on all desktops (user's screen). This image file contains the guest and host Operating System, applications, files and system settings of that particular desktop. A virtualization engine, mainly a Virtual Server, runs this VM and this VM behaves like a regular computer. The Virtual Machine is known as a host and it can be a user's desktop or a centralized server. A guest and host operating system must be installed on the VM image file so that files and resources can be shared efficiently and reliably between the user's desktops. For desktop virtualization, it is necessary to purchase the Virtual Server, thin-client devices and the virtualization software.

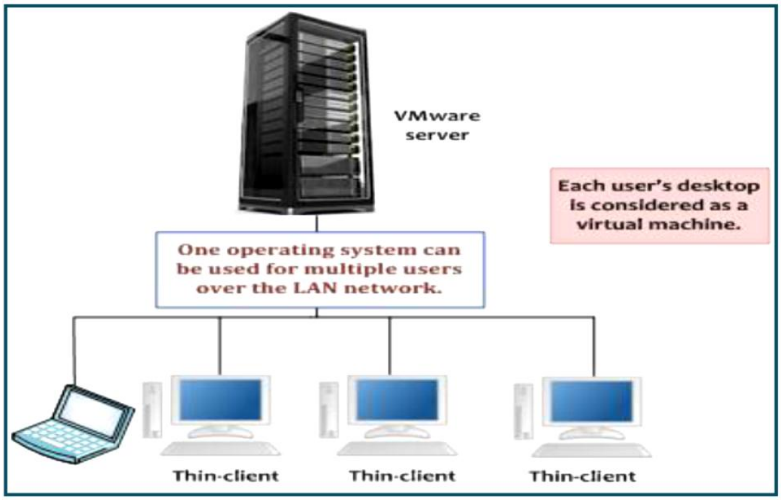

Figure 4: How virtual network works

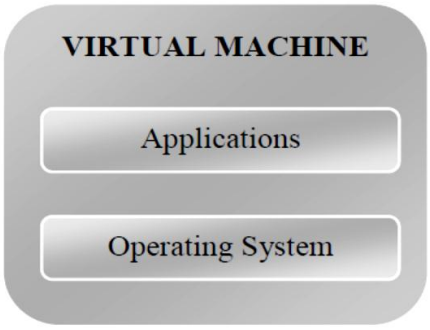

Figure 5**:** Virtual Machine (Sherlin, 2011)

4.0 Summary and Conclusion

The paper designs a thin-client network framework that overcome the identified challenges of client-server network which consisted of workstations, servers, networking components, and other shared resources that were facing security challenges. For instances, static IP which increases security risk and PC-Server network that has become difficult to maintain thereby resulting in high IT expenditure. Virtualized network emerged as the best thin-client computing

solution for organizations. This technology has many advantages over a traditional PC-server network: improved security, more reliable and available at all times giving users remote access, reduced IT support costs and support for number of applications and data. Another advantage of virtualization is that there is no need to replace the entire hardware and equipment with new ones except for an additional server, virtual server, which needs to be purchased so as to support virtualization. With virtualization, data and applications are centrally stored in the server and nothing needs to be saved in the client side. It is safe to say that this solution is capable of achieving the following: Centralized management of data and applications in a secure way, elimination of viruses, malwares and improved security

Refernces

Anwar, H and Xiaodi, H. 2012. An E-learning System Architecture Based on Cloud Computing. World Academy of Science, Engineering and Technology.

Barrie, D. 2002. Thin client benefits. ThinClient.net, p. 5. From: *http://www.thinclient.net/new_site/pdf/Thin_Client_Benefits_Paper.pdf.*

Carl, S. and Guynes, JW. 2011. Revisiting Client/Server Computing.

Cimen, C, Kavurucu, Y. and Aydin, H. 2014. Usage of thin-client / Server Architecture in Computer Aided Computing World Academy of Science, Engineering and Technology.

Davis, E. 2008. Green Benefits Put Thin-Client Computing Back on the Desktop Hardware Agenda, White, ForresterResearchInc.*http://www.hp.com/canada/products/landing/thin_clients/files/Forrestor -Green_and_TCs.pdf*

Deboosere, L, De Wachter, J, Simoens, P, De Turck, F, Dhoedt, B. and Demeester, P. 2007. Thin Client Computing Solutions in Low- and High-Motion Scenarios. In Third International Conference on Networkingand Services (ICNS), pages 38–38

Hatakeyama, Y., Kataoka, H., Nakajima, N., Watabe, T., Okuhara, Y., and Sagara, Y. 2011. An Education Support System with Anonymized Medical Data Based on Thin Client System

Internet of Things (iThings/CPSCom), 2011. International Conference on and 4th International Conference on Cyber, Physical and Social Computing, Page(s): 494 – 497.

Joel, K. 2005. Understanding Thin-Client/Server Computing.

Jonathon, M. and Robison, R. 2004. Network Security in a Thin Client (LTSP) Architecture

Lawton, C. 2007. Dumb terminals' can be a smart move. Wall Street Journal. from: *http://www.thinclient.net/new_site/pdf/Thin_Client_Benefits_Paper.pdf.*

Lee YH., Kim HS and Kim BK. 2015. Desktop Computer Virtualization for Improvement Security, Power Consumption and Cost by SBC (Server Based Computer). International Journal of Security and Its Applications Vol. 9, No. 5, pp. 141-152 ISSN: 1738-9984 IJSIA. http://dx.doi.org/10.14257/ijsia

Rajesh, P. and Umesh, K. 2012. An Overview and Study of Security Issues & Challenges in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 9, September 2012 ISSN: 2277 128X

Reynolds, G. 2006. Reducing IT Costs through the Design and Implementation of a Thin Client Infrastructure in Educational Environments. Irish Signals and Systems Conference. ET, Page(s): 73 – 78.

Robison, R, and Jonathon, M. 2004. Network Security in a Thin Client (LTSP) Architecture

Sherlin, V. 2011. Virtualization solution for health care organization.

Wyse Technology; Wyse S10 2007. Retrieved April 5, 2007, from Wyse Technology Products and Services Web site: *http://www.wyse.com/products*.

Yusuf, KC. and Halit, A. 2014. Usage of thin-client / server architecture in computer aided Education Turkish Public College, Tuzla, Istanbul, 34940, Turkey halitaydin81@dho.edu.tr